a b c d e f g h i j k l m n o p q r s t u v w x y z
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

18/5/24 APPLIED CRYPTOGRAPHY.

1). STREAM CIPHERS.

SUBSTITUTION

① Caesar cipher. - Mono

Q.1. Message: 'hello', key: 15

⇒ h - 7
e - 4
l - 11
l - 11
o - 14

$C_1 = (7+15)\%26 = 22 \rightarrow W$
$C_2 = (4+15)\%26 = 19 \rightarrow T$
$C_3 = (11+15)\%26 = 0 \rightarrow A$
$C_4 = (11+15)\%26 = 0 \rightarrow A$
$C_5 = (14+15)\%26 = 3 \rightarrow D$

Cipher text: WTAAD

Decryption

$W \rightarrow 22$	$P_1 = (22-15)\%26 = 7 \rightarrow H$
$T \rightarrow 19$	$P_2 = (19-15)\%26 = 4 \rightarrow E$
$A \rightarrow 0$	$P_3 = (0-15)\%26 = 11 \rightarrow L$
$A \rightarrow 0$	$P_4 = (0-15)\%26 = 11 \rightarrow L$
$D \rightarrow 3$	$P_5 = (3-15)\%26 = 14 \rightarrow O$

'If becoming -ve, add 26'

Plain text: HELLO.

→ Vulnerable to ciphertext-only attacks. Trying different keys might reveal the plaintext if key value is a small no.

② Affine Cipher. - Mono

Q.1. Message: hello,
$k_1 = 7$, $k_2 = 2$

Encrypt

h → 7 $T_1 = (7 * 7) \% 26 = 23$
e → 4 $T_2 = (4 * 7) \% 26 = 2$
l → 11 $T_3 = (11 * 7) \% 26 = 25$
l → 11 $T_4 = (11 * 7) \% 26 = 25$
o → 14 $T_5 = (14 * 7) \% 26 = 20$

$C_1 = (23 + 2) \% 26 = 25 \rightarrow Z$
$C_2 = (2 + 2) \% 26 = 4 \rightarrow E$
$C_3 = (25 + 2) \% 26 = 1 \rightarrow B$
$C_4 = (25 + 2) \% 26 = 1 \rightarrow B$
$C_5 = (20 + 2) \% 26 = 22 \rightarrow W$

Ciphertext: ZEBBW

Decrypt Find k_1^{-1} by hit and run method.

$(k_1 * x) \% 26 = 1$
$(7 * x) \% 26 = 1$
$x = 15$
$k_1^{-1} = 15$

$k_2 = 2$

$T_1 = (25 - 2) \% 26 = 23$
$T_2 = (4 - 2) \% 26 = 2$
$T_3 = (1 - 2) \% 26 = 25$
$T_4 = (1 - 2) \% 26 = 25$
$T_5 = (22 - 2) \% 26 = 20$

$P_1 = (23 * k^{-1}) \% 26 = (23 * 15) \% 26 = 7 \rightarrow H$
$P_2 = (2 * 15) \% 26 = 4 \rightarrow E$
$P_3 = (25 * 15) \% 26 = 11 \rightarrow L$
$P_4 = (25 * 15) \% 26 = 11 \rightarrow L$
$P_5 = (20 * 15) \% 26 = 14 \rightarrow O$

Plaintext: HELLO

Q.2. Msg: college $(k_1, k_2) = (17, 20)$

Encrypt:

c → 2	$T_1 = (2 * 17) \% 26 = 8$
o → 14	$T_2 = (14 * 17) \% 26 = 4$
l → 11	$T_3 = (11 * 17) \% 26 = 5$
l → 11	$T_4 = (11 * 17) \% 26 = 5$
e → 4	$T_5 = (4 * 17) \% 26 = 16$
g → 6	$T_6 = (6 * 17) \% 26 = 24$
e → 4	$T_7 = (4 * 17) \% 26 = 16$

$C_1 = (8 + 20) \% 26 = 2 \rightarrow C$
$C_2 = (4 + 20) \% 26 = 24 \rightarrow Y$
$C_3 = (5 + 20) \% 26 = 25 \rightarrow Z$
$C_4 = (5 + 20) \% 26 = 25 \rightarrow Z$
$C_5 = (16 + 20) \% 26 = 10 \rightarrow K$
$C_6 = (24 + 20) \% 26 = 18 \rightarrow S$
$C_7 = (16 + 20) \% 26 = 10 \rightarrow K$

Ciphertext: CYZZKSK

Decrypt: $(17 * x) \% 26 = 1$

$x = 23$

$k^{-1} = 23$

$(k_1^{-1}, k_2) = (23, 20)$

$T_1 = (2 - 20) \% 26 = 8$ $\quad P_1 = (8 * 23) \% 26 = 2 \rightarrow c$

$T_2 = (24 - 20) \% 26 = 4$ $\quad P_2 = (4 * 23) \% 26 = 14 \rightarrow o$

$T_3 = (25 - 20) \% 26 = 5$ $\quad P_3 = (5 * 23) \% 26 = 11 \rightarrow l$

$T_4 = (25 - 20) \% 26 = 5$ $\quad P_4 = (5 * 23) \% 26 = 11 \rightarrow l$

$T_5 = (10 - 20) \% 26 = 16$ $\quad P_5 = (16 * 23) \% 26 = 4 \rightarrow e$

$T_6 = (18 - 20) \% 26 = 24$ $\quad P_6 = (24 * 23) \% 26 = 6 \rightarrow g$

$T_7 = (10 - 20) \% 26 = 16$ $\quad P_7 = (16 * 23) \% 26 = 4 \rightarrow e$

Plain text : college.

Monoalphabetic substitution cipher: Each occurence of a letter will have the same substitution (in the same plaintext)

Polyalphabetic substitution cipher: Each occurence of a letter will have different substitutions.

(3) Vignere Cipher - Poly

Q.1. message: hello, key: test

Encrypt

h → 7	t → 19	$c_1 = (7+19)\%26 = 0 \rightarrow a$
e → 4	e → 4	$c_2 = (4+4)\%26 = 8 \rightarrow i$
l → 11	s → 18	$c_3 = (11+18)\%26 = 3 \rightarrow d$
l → 11	t → 19	$c_4 = (11+19)\%26 = 4 \rightarrow e$
o → 14	t → 19	$c_5 = (14+19)\%26 = 7 \rightarrow h$

Ciphertext: aideh

ecrypt $P_1 = (0-19)\%26 = 7 \rightarrow h$

$P_2 = (8-4)\%26 = 4 \rightarrow e$

$P_3 = (3-18)\%26 = 11 \rightarrow l$

$P_4 = (4-19)\%26 = 11 \rightarrow l$

$P_5 = (7-19)\%26 = 14 \rightarrow o$

Plaintext: hello

Attacks:

kasiski test → fourozan.

(4) Hill Cipher → Poly

Message = ATTACK

key mat = $\begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix}$

Encrypt: $P = \begin{bmatrix} A & T & C \\ T & A & K \end{bmatrix}$

$P_1 = \begin{bmatrix} 0 \\ 19 \end{bmatrix}$, $P_2 = \begin{bmatrix} 19 \\ 0 \end{bmatrix}$, $P_3 = \begin{bmatrix} 2 \\ 10 \end{bmatrix}$

$C_1 = \begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix} \begin{bmatrix} 0 \\ 19 \end{bmatrix} \%26 = \begin{bmatrix} 57 \\ 114 \end{bmatrix} \%26 = \begin{bmatrix} 5 \\ 10 \end{bmatrix} = \begin{bmatrix} F \\ K \end{bmatrix}$

$C_2 = \begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix} \begin{bmatrix} 19 \\ 0 \end{bmatrix} \%26 = \begin{bmatrix} 38 \\ 57 \end{bmatrix} \%26 = \begin{bmatrix} 12 \\ 5 \end{bmatrix} = \begin{bmatrix} M \\ F \end{bmatrix}$

$C_3 = \begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix} \begin{bmatrix} 2 \\ 10 \end{bmatrix} \%26 = \begin{bmatrix} 34 \\ 66 \end{bmatrix} \%26 = \begin{bmatrix} 8 \\ 14 \end{bmatrix} = \begin{bmatrix} I \\ O \end{bmatrix}$

$$C = \begin{bmatrix} F & M & I \\ K & F & O \end{bmatrix}$$

Ciphertext: FKMFIO

Decrypt: $\text{key} = \begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix}$

$|m| = 12 - 9 = 3$

Mat is invertible

$\therefore \quad m^{-1} = \frac{1}{|m|} \text{adj} M$

$$\text{adj} m = \begin{bmatrix} 6 & -3 \\ -3 & 2 \end{bmatrix} \approx \begin{bmatrix} 6 & 23 \\ 23 & 2 \end{bmatrix}$$

To find $|m|^{-1}$,

$(|m| * x) \% 26 = 1$

$(3 * x) \% 26 = 1$

$x = 9$

$$\therefore \quad m^{-1} = \left(9 * \begin{bmatrix} 6 & -3 \\ -3 & 2 \end{bmatrix}\right) \% 26$$

$$= \begin{bmatrix} 54 & -27 \\ -27 & 18 \end{bmatrix} \% 26$$

Add 26 to the negative value

$$m^{-1} = \left(9 * \begin{bmatrix} 6 & 23 \\ 23 & 2 \end{bmatrix}\right) \% 26$$

$$m^{-1} = \begin{bmatrix} 54 & 207 \\ 207 & 18 \end{bmatrix} \% 26 = \begin{bmatrix} 2 & 25 \\ 25 & 18 \end{bmatrix}$$

$$C = \begin{bmatrix} F & M & I \\ K & P & O \end{bmatrix}$$

$$C_1 = \begin{bmatrix} F \\ K \end{bmatrix} = \begin{bmatrix} 5 \\ 10 \end{bmatrix}, \quad C_2 = \begin{bmatrix} M \\ P \end{bmatrix} = \begin{bmatrix} 12 \\ 5 \end{bmatrix}, \quad C_3 = \begin{bmatrix} I \\ O \end{bmatrix} = \begin{bmatrix} 8 \\ 14 \end{bmatrix}$$

$$\therefore P_1 = \begin{bmatrix} 2 & 25 \\ 25 & 18 \end{bmatrix} \begin{bmatrix} 5 \\ 10 \end{bmatrix} \% 26 = \begin{bmatrix} 0 \\ 19 \end{bmatrix} = \begin{bmatrix} A \\ T \end{bmatrix}$$

$$P_2 = \begin{bmatrix} 2 & 25 \\ 25 & 18 \end{bmatrix} \begin{bmatrix} 12 \\ 5 \end{bmatrix} \% 26 = \begin{bmatrix} 19 \\ 0 \end{bmatrix} = \begin{bmatrix} T \\ A \end{bmatrix}$$

$$P_3 = \begin{bmatrix} 2 & 25 \\ 25 & 18 \end{bmatrix} \begin{bmatrix} 8 \\ 14 \end{bmatrix} \% 26 = \begin{bmatrix} 2 \\ 10 \end{bmatrix} = \begin{bmatrix} C \\ K \end{bmatrix}$$

$$P = \begin{bmatrix} A & T & C \\ T & A & K \end{bmatrix}$$

Plaintext: ATTACK.

Cryptanalysis of Hill cipher.

→ Ciphertext only attack is difficult to execute on hill cipher.

→ Hill cipher don't preserve statistics of the plaintext. Attacker can't run frequency analysis on single letters, digrams or trigrams.

→ Known plaintext attack might be poss if the knows value of m and ciphertext-plaintext pairs for atleast m blocks. Blocks may belong to same or different messages.

$$C = PK,$$

$$K = CP^{-1}$$

Encryption: Always enter → rowwise
readoff → columnwise

Decryption:
Enter columnwise
Readoff rowwise

TRANSPOSITION

① Columnar Transposition

Q-1. Message: kill corona virus at twelve am tomorrow
key: 4312567

Encrypt

4	3	1	2	5	6	7
k	i	l	l	c	o	r
o	n	a	v	i	r	u
s	a	t	t	w	e	l
v	e	a	m	t	o	m
o	r	r	o	w		

Ciphertext: latar lvtmo inaer kosvo ciwtw orc rulm

~~Decrypt:~~

1	7
v	a
t	t
m	a
o	r

Decrypt:

4	3	1	2	5	6	7
k	i	l	l	c	o	r
o	n	a	v	i	r	u
s	a	t	t	w	e	l
v	e	a	m	t	o	m
o	r	r	o	w		

{For decryption, write the words in the ciphertext in the column of the no. with their position no.}

Plain text: kill corona virus at twelve am tomorrow

Q.2. Message: ENEMYATTACKSTONIGHT
Key: 3 1 4 5 2

Encrypt

3	1	4	5	2
E	N	E	M	Y
A	T	T	A	C
K	S	T	O	N
I	G	H	T	

Ciphertext: NTSG YCN EAKI ETTH MAOT

Decrypt

3	1	4	5	2
E	N	E	M	Y
A	T	T	A	C
K	S	T	O	N
I	G	H	T	

Plaintext: ENEMY ATTACKS TONIGHT

(2) Rail Fence.

Q.1. Message: HAPPY BIRTHDAY TO YOU
Depth=2

Encrypt

H		P		Y		I		T		D		Y		O		O		U
	A		P		B		R		H		A		T		Y		U	

Ciphertext: HPYITDYOO APBRHATYU

Decrypt

H		P		Y		I		T		D		Y		O		O		U
	A		P		B		R		H		A		T		Y		U	

plaintext: HAPPY BIRTHDAY TO YOU

③ Playfair

1) Plain text: attack
Keyword: monarch

Same column → down
Same row → right
Quadrilateral → opposite corners.

m	o	n	a	r
c	h	b	d	e
f	g	i/j	k	l
p	q	s	t	u
v	w	x	y	z

at ta ck
↓ ↓ ↓
dy yd df

ciphertext: dyyddf

Decrypt

m	o	n	a	r
c	h	b	d	e
f	g	i/j	k	l
p	q	s	t	u
v	w	x	y	z

dy yd df
↓ ↓ ↓
at ta ck

plaintext: attack.

Always,
→ The shape for compression
→ The shape per expansion

Q.2. key: moonmission If same letters in diagraph, append x.
plaintext: greet

Encrypt

m	o	n	i/j	s
a	b	c	d	e
f	g	h	k	l
p	q	r	t	u
v	w	x	y	z

gr ex et
↓ ↓ ↓
hq cz du

Ciphertext: hqczdu

Decrypt

m	o	n	i/j	s
a	b	c	d	e
f	g	h	k	l
p	q	r	t	u
v	w	x	y	z

hq cz du
↓ ↓ ↓
gr ex et

Plaintext: greet

Q.3. Plaintext: why don't you
keyword: keyword

Encrypt

k	e	y	w	o
r	d	a	b	c
f	g	h	i/j	l
m	n	p	q	s
t	u	v	x	z

wh yd on ty ou
↓ ↓ ↓ ↓ ↓
yi ea es ez
VF

ciphertext: yieaestvez

Decrypt

k	e	y	w	o
r	d	a	b	c
f	g	h	i/j	l
m	n	p	q	s
t	u	v	x	z

yi ea es tv ez
↓ ↓ ↓ ↓ ↓
wh yd on ty ou

Plaintext: why don't you.

2) BLOCK CIPHERS.

1) AES
2) Mix-column operation, key generation.

Q-1. State: $\begin{bmatrix} D & J \\ S & C \end{bmatrix}$

Const mat = $\begin{bmatrix} 01 & 02 \\ 02 & 03 \end{bmatrix}$

A - 00
B - 01
C - 02
D - 03
E - 04
F - 05
G - 06
H - 07
I - 08
J - 09
K - 0A
L - 0B
M - 0C
N - 0D
O - 0E
P - 0F
Q - 10
R - 11
S - 12
T - 13
U - 14
V - 15
W - 16
X - 17
Y - 18
Z - 19

State = $\begin{bmatrix} 03 & 09 \\ 12 & 02 \end{bmatrix}$

$$\begin{bmatrix} b0 & b2 \\ b1 & b3 \end{bmatrix} = \begin{bmatrix} 01 & 02 \\ 02 & 03 \end{bmatrix} \begin{bmatrix} 03 & 09 \\ 12 & 02 \end{bmatrix}$$

$$\begin{bmatrix} b0 \\ b1 \end{bmatrix} = \begin{bmatrix} 01 & 02 \\ 02 & 03 \end{bmatrix} \begin{bmatrix} 03 \\ 12 \end{bmatrix}$$

$b0 = (01 * 03) \oplus (02 * 12)$

$b1 = (02 * 03) \oplus (03 * 12)$

01 → 0000 0001

03 → 0000 0011

$x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$

{01} 0 0 0 0 0 0 0 1

{01} = 1

{03} 0 0 0 0 0 0 1 1

{03} = x + 1

(01 * 03) = (x + 1)

= 0000 0011

(01 * 03) = 03

02 → 0000 0010

12 → 0001 0010

$x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$

{02} 0 0 0 0 0 0 1 0

{02} = x

{12} = 0 0 0 1 0 0 1 0

$= x^4 + x$

$\{02 * 12) = x(x^4 + x) = x^5 + x^2$

(02 * 12) = 0010 0100

(02 * 12) = 24

(01 * 03) ⊕ (02 * 12) = 03 ⊕ 24

= 0000 0011 ⊕ 0010 0100

= 0010 0111

b0 = (01 * 03) ⊕ (02 * 12) = 27

02 → 0000 0010

03 → 0000 0011

$x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$

{02} = 0 0 0 0 0 0 1 0

{02} = x

{03} 0 0 0 0 0 0 1 1

{03} = x + 1

(02 * 03) = x(x + 1) = $x^2 + x$

(02 * 03) = 0000 0110 = 06

03 → 0000 0011

12 → 0001 0010

$x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$

{03} = 0 0 0 0 0 0 1 1

{03} = x + 1

{12} 0 0 0 1 0 0 1 0

{12} = $x^4 + x$

(03 * 12) = $(x+1)(x^4+x) = x^5 + x^2 + x^4 + x$ = ~~0000 0~~

= 0011 0110

(03 * 12) = 36

(02 * 03) ⊕ (03 * 12) = 06 ⊕ 36 = 0000 0110 ⊕ 0011 0110

= 0011 0000

(02 * 03) ⊕ (03 * 12) = 30

$b_1 = (02 * 03) \oplus (03 * 12) = 30$

$$\begin{bmatrix} b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} 01 & 02 \\ 02 & 03 \end{bmatrix} \begin{bmatrix} 09 \\ 02 \end{bmatrix}$$

$b_2 = (01 * 09) \oplus (02 * 02)$

$b_3 = (02 * 09) \oplus (03 * 02)$

01 → 0000 0001

09 → 0000 1001

$x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$

{01} = 0 0 0 0 0 0 0 1

{01} = 1

{09} 0 0 0 0 1 0 0 1

{09} = $x^3 + 1$

$(01 * 09) = x^3 + 1 = 0000\ 1001 = 09$

02 → 0000 0010

$x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$

{02} 0 0 0 0 0 0 1 0

{02} = x

$(02 * 02) = x^2 = 0000\ 0100 = 04$

$(01 * 09) \oplus (02 * 02) = 09 \oplus 04 = 0000\ 1001 \oplus 0000\ 0100$

$= 0000\ 1101$

$b_2 = (01 * 09) \oplus (02 * 02) = 0D$

02 → 0000 0010

09 → 0000 1001

$x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$

{02} = 0 0 0 0 0 0 1 0

{02} = x

$$x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$$

{09} = 0 0 0 0 1 0 0 1

{09} = $x^3 + 1$

$(02 * 09) = x(x^3+1) = x^4 + x = 0001\ 0010 = 12$

{03} → 0000 0011

02 → 0000 0010

$$x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$$

{03} = 0 0 0 0 0 0 1 1

{03} = $x + 1$

{02} 0 0 0 0 0 0 1 0

{02} = x

$(03 * 02) = (x+1)x = x^2 + x = 0000\ 0110 = 06$

$(03 * 02) = 06$

$(02 * 09) \oplus (03 * 02) = 12 \oplus 06 = 0001\ 0010 \oplus 0000\ 0110$

$= 0001\ 0100$

$= 14$

$b_3 = (02 * 09) \oplus (03 * 02)$

$$\therefore \begin{bmatrix} b_0 & b_2 \\ b_1 & b_3 \end{bmatrix} = \begin{bmatrix} 27 & 0D \\ 30 & 14 \end{bmatrix}$$

Shift row opr

0 shift
1 shift
2 shifts
3 shifts

$$\begin{bmatrix} 63 & 47 & a2 & f0 \\ f2 & 9c & 63 & 65 \\ f0 & ab & 7b & 7c \\ af & 76 & 76 & ca \end{bmatrix} = \begin{bmatrix} 63 & 47 & a2 & f0 \\ 9c & 63 & 65 & f2 \\ 7b & 7c & f0 & ab \\ ca & af & 76 & 76 \end{bmatrix}$$

Q-2. $S = \begin{bmatrix} 63 & 47 \\ f2 & ac \end{bmatrix}$

$$C = \begin{bmatrix} 02 & 03 \\ 01 & 02 \end{bmatrix}$$

Soln $\begin{bmatrix} b_0 & b_2 \\ b_1 & b_3 \end{bmatrix} = \begin{bmatrix} 02 & 03 \\ 01 & 02 \end{bmatrix} \begin{bmatrix} 63 & 47 \\ f2 & ac \end{bmatrix}$

$$\begin{bmatrix} b_0 \\ b_1 \end{bmatrix} = \begin{bmatrix} 02 & 03 \\ 01 & 02 \end{bmatrix} \begin{bmatrix} 63 \\ f2 \end{bmatrix}$$

$b_0 = (02 * 63) \oplus (03 * f2)$

$b_1 = (01 * 63) \oplus (02 * f2)$

$02 \rightarrow 0000\ 0010$

$63 \rightarrow 0110\ 0011$

$x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$

$\{02\} = 0\ 0\ 0\ 0\ 0\ 0\ 1\ 0$

$\{02\} = x$

$\{63\}\ 0\ 1\ 1\ 0\ 0\ 0\ 1\ 1$

$\{63\} = x^6 + x^5 + x + 1$

$(02 * 63) \equiv x(x^6 + x^5 + x + 1) = x^7 + x^6 + x^2 + x = 1100\ 0110$

$= C6$

03 → 0000 0011

f2 → 1111 0010

$x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$

{03} = 0 0 0 0 0 0 1 1

{03} = x + 1

{f2} = 1 1 1 1 0 0 1 0

{f2} = $x^7 + x^6 + x^5 + x^4 + x$

(03 * f2) = $(x+1)(x^7 + x^6 + x^5 + x^4 + x)$ =

= $x^8 + x^7 + x^6 + x^5 + x^2 + x^7 + x^6 + x^5 + x^4 + x$

= $x^8 + x^4 + x^2 + x$

① g(x) = 100010110

p(x) = $x^8 + x^4 + x^3 + x + 01$ ← Irreducible polynomial

= 100011011

t(x) = g(x)/p(x) = 00000 0110 1

= 0000 1101

(03 * f2) = 0D

(02 * 63) ⊕ (03 * f2) = C6 ⊕ 0D = 1100 0110 ⊕ 0000 1101

= 1100 1011

$\boxed{b_0 = (02 * 63) \oplus (03 * f2) = CB}$

(01 * 63) = 63 → 0110 0011

02 → 0000 0010

f2 → 1111 0010

$x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$

$\{02\} = 0\ 0\ 0\ 0\ 0\ 0\ 1\ 0$

$\{02\} = x$

$\{f2\} = 1\ 1\ 1\ 1\ 0\ 0\ 1\ 0$

$\{f2\} = x^7 + x^6 + x^5 + x^4 + x$

$(02 * f2) = x(x^7 + x^6 + x^5 + x^4 + x) = x^8 + x^7 + x^6 + x^5 + x^2$

$(02 * f2) = 111100100$

$g(x) = 111100100$

$p(x) = x^8 + x^4 + x^3 + x + 1$

$p(x) = 100011011$

$t(x) = g(x) / p(x) = 011111111$

$= 1111\ 1111$

$(02 * f2) = ff$

$b_1 = (01 * 63) \oplus (02 * f_2) = 63 \oplus ff = 0110\ 0011 \oplus 1111\ 1111$

$= 1001\ 1100$

$\boxed{b_1 = (01 * 63) \oplus (02 * f_2) = 9C}$

$$\begin{bmatrix} b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} 02 & 03 \\ 01 & 02 \end{bmatrix} \begin{bmatrix} 47 \\ ac \end{bmatrix}$$

$b_2 = (02 * 47) \oplus (03 * ac)$

$b_3 = (01 * 47) \oplus (02 * ac)$

$02 \rightarrow 0000\ 0010$

$47 \rightarrow 0100\ 0111$

$x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$

$\{02\} = 0\ 0\ 0\ 0\ 0\ 0\ 1\ 0$

$\{02\} = x$

$\{47\} = 0\ 1\ 0\ 0\ 0\ 1\ 1\ 1$

$\{47\} = x^6 + x^2 + x + 1$

$(02 * 47) = x(x^6 + x^2 + x + 1) = x^7 + x^3 + x^2 + x = 1000\ 1110$

$(02 * 47) = 8E$

$03 \rightarrow 0000\ 0011$

$ac \rightarrow 1010\ 1100$

$x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$

$\{03\}y = 0\ 0\ 0\ 0\ 0\ 0\ 1\ 1$

$\{03\}y = x + 1$

$\{ac\}y = 1\ 0\ 1\ 0\ 1\ 1\ 0\ 0$

$\{ac\}y = x^7 + x^5 + x^3 + x^2$

$(03 * ac) = (x+1)(x^7 + x^5 + x^3 + x^2) = (x^8 + x^6 + x^4 + x^3) + (x^7 + x^5 + x^3 + x^2)$

$= x^8 + x^7 + x^6 + x^5 + x^2$

$(03 * ac) = 111100100$

$p(x) = x^8 + x^4 + x^3 + x + 1 = 100011011$

$t(x) = g(x)/p(x)$

$t(x) = 01111\ 1111 = ff$

$(03 * ac) = ff$

$(02 * 47) \oplus (03 * ac) = 8E \oplus FF = 1000\ 1110 \oplus 1111\ 1111$

$= 0111\ 0001$

$\boxed{b_2 = (02 * 47) \oplus (03 * ac) = 71}$

$01 * 47 = 47 \rightarrow 0100\ 0111$

$02 \rightarrow 0000\ 0010$

$ac \rightarrow 1010\ 1100$

$x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$

$\{02\}y = 0\ 0\ 0\ 0\ 0\ 0\ 1\ 0$

$\{02\}y = x$

$\{ac\}y = 1\ 0\ 1\ 0\ 1\ 1\ 0\ 0$

$\{ac\}y = x^7 + x^5 + x^3 + x^2$

$(02 * ac) = x(x^7 + x^5 + x^3 + x^2) = x^8 + x^6 + x^4 + x^3$

$g(x) = 101011000$

$p(x) = x^8 + x^4 + x^3 + x + 1 = 100011011$

$t(x) = g(x) \mid p(x)$

$(02 * ac) = 00100011 = 0100\ 0011 = 43$

$(02 * ac) = 43$

$(01 * 47) \oplus (02 * ac) = 47 \oplus 43$

$= 0100\ 0111 \oplus 0100\ 0011$

$= 0000\ 0100$

$b_3 = (01 * 47) \oplus (02 * ac) = 04$

$$\begin{bmatrix} b_0 & b_2 \\ b_1 & b_3 \end{bmatrix} = \begin{bmatrix} CB & 71 \\ 9C & 04 \end{bmatrix}$$

② Key Generation

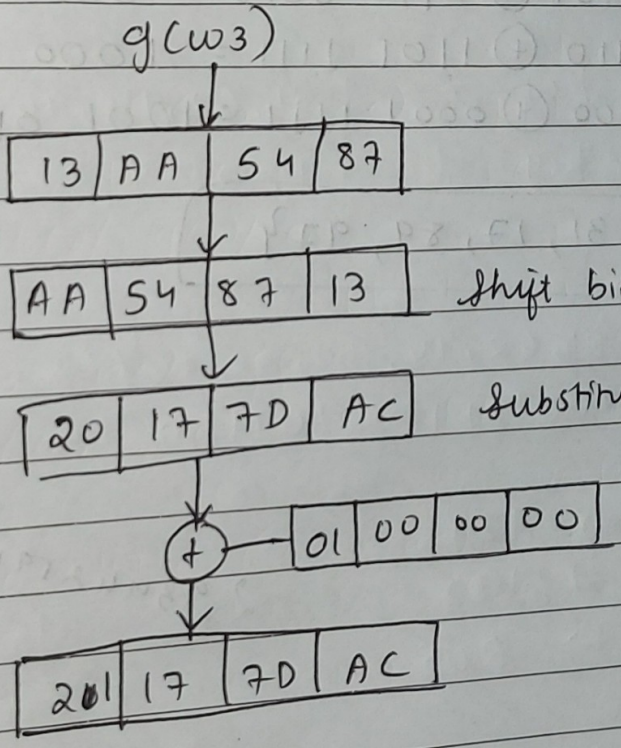
$w_4 = w_0 \oplus g(w_3)$
$w_5 = w_1 \oplus w_4$
$w_6 = w_2 \oplus w_5$
$w_7 = w_3 \oplus w_6$

Q.1. Generate w_4, w_5

$w_0 = \{24, 75, A2, B3\}$
$w_1 = \{34, 75, 56, 88\}$
$w_3 = \{13, AA, 54, 87\}$

S-Box

13	AA	54	87
AC	20	17	7D



$x_1 = 20 \oplus 01 = 0010\ 0000 \oplus 0000\ 0001 = 0010\ 0001 = 21$
$x_2 = 17 \oplus 00 = 0001\ 0111 \oplus 0000\ 0000 = 0001\ 0111 = 17$
$x_3 = 7D \oplus 00 = 0111\ 1101 \oplus 0000\ 0000 = 0111\ 1101 = 7D$
$x_4 = AC \oplus 00 = 1010\ 1100 \oplus 0000\ 0000 = 1010\ 1100 = AC$

$w_4 = w_0 \oplus g(w_3) = \{24, 75, A2, B3\} \oplus \{21, 17, 7D, AC\}$

$24 \oplus 21 = 0010\ 0100 \oplus 0010\ 0001 = 0000\ 0101 = 05$
$75 \oplus 17 = 0111\ 0101 \oplus 0001\ 0111 = 0110\ 0010 = 62$
$A2 \oplus 7D = 1010\ 0010 \oplus 0111\ 1101 = 1101\ 1111 = DF$
$B3 \oplus AC = 1011\ 0011 \oplus 1010\ 1100 = 0001\ 1111 = 1F$

$w_4 = \{05, 62, DF, 1F\}$

$w_5 = w_1 \oplus w_4$
$= \{34, 75, 56, 88\} \oplus \{05, 62, DF, 1F\}$

$34 \oplus 05 = 0011\ 0100 \oplus 0000\ 0101 = 0011\ 0001 = 31$
$75 \oplus 62 = 0111\ 0101 \oplus 0110\ 0010 = 0001\ 0111 = 17$
$56 \oplus DF = 0101\ 0110 \oplus 1101\ 1111 = 1000\ 1001 = 89$
$88 \oplus 1F = 1000\ 1000 \oplus 0001\ 1111 = 1001\ 0111 = 97$

$w_5 = \{31, 17, 89, 97\}$

$2.9344259 17 \times 10^{50}$

3) PUBLIC KEY CRYPTOGRAPHY (ASYMMETRIC CIPHERS)

① RSA

Q-1. $p = 3, q = 11$ $M = 31$

$n = pq = 33$

$\phi(n) = (p-1)*(q-1) = 20$

$e = \gcd(e, \phi(n)) = 1$

$e = 7$

$(d * e) \bmod 20 = 1$

$(d * e) \bmod 20 = 1$

$(d * 7) \bmod 20 = 1$

$d = 3$

Encryption:

$C = M^e \bmod n$

$= 31^7 \bmod 33$

$C = 4$

Decryption

$M = C^d \bmod n$

$= 4^3 \bmod 33$

$M = 31$

Encryption

$C = M^e \bmod n$

$= 5^{13} \bmod 77 = 26$

$C = 26$

Decryption

$M = C^d \bmod n$

$= 26^{37} \bmod 77 =$

$M = 5$

using $e = 7$

$(d * e) \bmod \phi(n) = 1$

$(d * 7) \bmod 60 = 1$

Q.2. $p = 7, q = 11$, $M = 5$

$n = pq = 77$

$\phi(n) = (p-1)*(q-1) = 60$

$e = \gcd(e, \phi(n)) = 1$

$e = 13$

$(d * e) \bmod \phi(n) = 1$

$(d * 13) \bmod 60 = 1$

$d = 37$

② Knapsack.

Q-1. Superincer = {1, 2, 4, 10, 20, 40}

m = 110

gcd(m, n) = 1

n = 31

Key Generation

(1 * 31) mod 110 = 31

(2 * 31) mod 110 = 62

(4 * 31) mod 110 = 14

(10 * 31) mod 110 = 90

(20 * 31) mod 110 = 70

(40 * 31) mod 110 = 30

Public key = e = {31, 62, 14, 90, 70, 30}

Private key = d = {1, 2, 4, 10, 20, 40}

Encryption

e = {31, 62, 14, 90, 70, 30}

m = 100100 111100 101110

100100 → 121

111100 → 197

101110 → 205

c = {121, 197, 205}

Decryption.

(x * n) % 110 = 1

(x * 31) mod 110 = 1

x = 71

$(121 * 71) \bmod 110 = 11$

$(97 * 71) \bmod 110 = 17$

$(205 * 71) \bmod 110 = 35$

$d = \{1, 2, 4, 10, 20, 40\}$

11 — 1 0 0 1 0 0

17 — 1 1 1 1 0 0

35 — 1 0 1 1 1 0

$M = 100100\ 111100\ 101110$

2. $M = 1100$

super incr $= \{1, 2, 4, 10\}$

$m = 20$

$\gcd(m, n) = 1$

$n = 7$

Key generation

$(1 * 7) \bmod 20 = 7$

$(2 * 7) \bmod 20 = 14$

$(4 * 7) \bmod 20 = 8$

$(10 * 7) \bmod 20 = 10$

$e = \{7, 14, 8, 10\}$

$d = \{1, 2, 4, 10\}$

Encryption

$e = \{7, 14, 8, 10\}$

$c = 21$

Decryption

$(x * n) \bmod 20 = 1$

$(7 * x) \bmod 20 = 1$

$x = 3$

$(21 * 3) \bmod 20 = 3$

$d = \{1, 2, 4, 10\}$

$M = 1100$

4) KEY EXCHANGE ALGORITHM

Diffie Hellman.

Q-1. $p = 11$

$2^1 \bmod 11 = 2$
$2^2 \bmod 11 = 4$
$2^3 \bmod 11 = 8$
$2^4 \bmod 11 = 5$
$2^5 \bmod 11 = 10$
$2^6 \bmod 11 = 9$
$2^7 \bmod 11 = 7$
$2^8 \bmod 11 = 3$
$2^9 \bmod 11 = 6$
$2^{10} \bmod 11 = 1$

$\boxed{\alpha = 2}$

$x_A = 5$ $\quad x_B = 3$

$y_A = \alpha^{x_A} \bmod p$
$y_A = 2^5 \bmod 11$
$y_A = 10$

$y_B = \alpha^{x_B} \bmod p$
$y_B = 2^3 \bmod 11$
$y_B = 8$

$k_1 = y_B^{x_A} \bmod p$
$= (8)^5 \bmod 11$
$k_1 = 10$

$k_2 = y_A^{x_B} \bmod p$
$= (10)^3 \bmod 11$
$k_2 = 10$

$\boxed{k_1 = k_2}$

Q-2. $p = 7$

$2^1 \bmod 7 = 2$
$2^2 \bmod 7 = 4$
$2^3 \bmod 7 = 1$
$2^4 \bmod 7 = 2$
X

$3^1 \bmod 7 = 3$
$3^2 \bmod 7 = 2$
$3^3 \bmod 7 = 6$
$3^4 \bmod 7 = 4$
$3^5 \bmod 7 = 5$
$3^6 \bmod 7 = 1$
~~$3^7 \bmod$~~

$\alpha = 3$

$x_A = 3$, $\quad x_B = 5$

$y_A = \alpha^{x_A} \bmod p$
$= (3)^3 \bmod 7$
$y_A = 6$

$y_B = \alpha^{x_B} \bmod p$
$= (3)^5 \bmod 7$
$y_B = 5$

$k_1 = y_B^{x_A} \bmod p$
$= (5)^3 \bmod 7$
$k_1 = 6$

$k_2 = y_A^{x_B} \bmod p$
$= (6)^5 \bmod 7$
$k_2 = 6$

$k_1 = k_2$.